Claims

What is claimed is:

1. In a call processing system, a method for providing secure communications between two or more end units of the system via a communication switch of the system, the method comprising the steps of:

storing in a memory associated with the communication switch a plurality of sets of session key lists including a set of session key lists for each of the end units;

selecting as an end unit to end unit session key a session key from a session key list in a given one of the sets of session key lists associated with an originating end unit, the selected end unit to end unit session key being utilizable in providing secure communications between the originating end unit and at least one other end unit via the communication switch.

2. The method of claim 1 wherein the given one of the sets of session key lists is stored in the form of a data structure comprising at least a first session key element and a plurality of stack-based session key lists, each of the stack-based session key lists comprising a plurality of session keys associated with a particular terminal coupled to the originating end unit.

3. The method of claim 2 wherein the first session key element is utilizable in providing secure communication between the originating end point and the communication switch.

4. The method of claim 2 wherein the selected session key is selected from a designated one of the plurality of stack-based session key lists corresponding to a particular terminal which originated the secure communications via the originating end unit.

5. The method of claim 4 wherein upon completion of the secure communications originated by the particular terminal, the corresponding originating end unit generates at least one additional session key which is added to the stack-based session key list for that terminal and is supplied to the communication switch for storage, the additional session key being utilizable in providing subsequent secure communications between the originating end unit and at least one other end unit.

6. The method of claim 1 wherein the set of session key lists for a given one of the end units is supplied to the communication switch in encrypted form by that end unit as part of an authentication protocol carried out between that end unit and the communication switch.

7. The method of claim 1 wherein a first session key element of the set of session key lists is utilizable for providing secure communications between the given one of the end units and the communication switch subsequent to completion of the authentication protocol.

8. The method of claim 1 wherein a particular one of the session key lists associated with a particular terminal coupled to the originating end unit is selected for use in providing secure communications for a call originating at the particular terminal.

9. The method of claim 8 wherein at least one additional terminal coupled to another end unit utilizes the selected session key to participate in the call originating at the particular terminal.

10. The method of claim 9 wherein the additional terminal comprises a corresponding destination terminal of the call originating at the particular terminal.

11. The method of claim 9 wherein the additional terminal comprises an additional terminal other than a destination terminal of the call, the additional terminal being conferenced into the call originating at the particular terminal subsequent to connection of the call to the destination terminal.

12. The method of claim 11 wherein a new session key is selected from the session key list associated with the particular terminal after the additional terminal conferenced into the call is subsequently dropped from the call.

13. An apparatus for use in a call processing system for providing secure communications between two or more end units of the system via a communication switch of the system, the apparatus comprising:

a memory associated with the communication switch and operative to store a plurality of sets of session key lists including a set of session key lists for each of the end units; and

a processor coupled to the memory, the processor being operative to select as an end unit to end unit session key a session key from a session key list in a given one of the sets of session key lists associated with an originating end unit, the selected end unit to end unit session key being utilizable in providing secure communications between the originating end unit and at least one other end unit via the communication switch.

14. The apparatus of claim 13 wherein the given one of the sets of session key lists is stored in the form of a data structure comprising at least a first session key element and a plurality of stack-based session key lists, each of the stack-based session key lists comprising a plurality of session keys associated with a particular terminal coupled to the originating end unit.

15. The apparatus of claim 14 wherein the first session key element is utilizable in providing secure communication between the originating end point and the communication switch.

16. The apparatus of claim 14 wherein the selected session key is selected from a designated one of the plurality of stack-based session key lists corresponding to a particular terminal which originated the secure communications via the originating end unit.

17. The apparatus of claim 16 wherein upon completion of the secure communications originated by the particular terminal, the corresponding originating end unit generates at least one additional session key which is added to the stack-based session key list for that terminal and is supplied to the communication switch for storage, the additional session key being utilizable in providing subsequent secure communications between the originating end unit and at least one other end unit.

18. The apparatus of claim 13 wherein the set of session key lists for a given one of the end units is supplied to the communication switch in encrypted form by that end unit as part of an authentication protocol carried out between that end unit and the communication switch.

19. The apparatus of claim 13 wherein a first session key element of the set of session key lists is utilizable for providing secure communications between the given one of the end units and the communication switch subsequent to completion of the authentication protocol.

20. The apparatus of claim 13 wherein a particular one of the session key lists associated with a particular terminal coupled to the originating end unit is selected for use in providing secure communications for a call originating at the particular terminal.

21. The apparatus of claim 20 wherein at least one additional terminal coupled to another end unit utilizes the selected session key to participate in the call originating at the particular terminal.

22. The apparatus of claim 21 wherein the additional terminal comprises a corresponding destination terminal of the call originating at the particular terminal.

23. The apparatus of claim 21 wherein the additional terminal comprises an additional terminal other than a destination terminal of the call, the additional terminal being conferenced into the call originating at the particular terminal subsequent to connection of the call to the destination terminal.

24. The apparatus of claim 23 wherein a new session key is selected from the session key list associated with the particular terminal after the additional terminal conferenced into the call is subsequently dropped from the call.

25. An article of manufacture comprising a machine-readable storage medium storing one or more programs for use in a call processing system for providing secure communications between two or more end units of the system via a communication switch of the system, wherein the one or more programs when executed implement the steps of:

storing in a memory associated with the communication switch a plurality of sets of session key lists including a set of session key lists for each of the end units;

selecting as an end unit to end unit session key a session key from a session key list in a given one of the sets of session key lists associated with an originating end unit, the selected end unit to end unit session key being utilizable in providing secure communications between the originating end unit and at least one other end unit via the communication switch.